Salem Public Library

The Resilient Library Newsletter

January 31, 2021 Volume 4, Issue 5

PLEASE NOTE:

Many of the images and underlined text in this newsletter have hyperlinks to their corresponding websites

Click (or Ctrl-click) on images and un-der-lined text to be directed to those websites

Inside this issue:

2021 Online Tax Preparation Products to Offer Multi-Factor Authentication

WASHINGTON — The Internal Revenue Service, state tax agencies and the tax industry today marked the second day of National Tax Security Awareness Week by announcing an improved feature that will be available on all 2021 online tax preparation products.

Designed to protect both taxpayers and tax professionals, multi-factor authentication means the returning user must enter two pieces of data to securely access an account or application. For example, taxpayers must enter their credentials (username and password) plus a numerical code sent as a text to their mobile phone.

The agreement to add the multi-factor authentication feature is just one publicly visible example of the ongoing collaboration by the IRS, state tax agencies and the tax industry, which work together as the Security Summit. 2020 marks the fifth year of the Security Summit and of National Tax Security Awareness Week.

"Multi-factor authentication option is an easy, free way to really step up protection of your data whether you're a taxpayer or a tax professional," said Chuck Rettig, IRS Commissioner. "This is an important step being taken by the tax software industry. This is just one example of the many actions taken by the Summit partners over the past five years that have dramatically improved our ability to combat identity thieves and to protect taxpayers."

Some online products previously offered multi-factor authentication. However, for 2021 all providers agreed to make it a standard feature and all agreed that it would meet requirements set by the National Institute of Standards and Technology. Multi-factor authentication may not be available on over-the-counter hard disk tax products.

Because the multi-factor authentication option is voluntary, Summit partners urged both taxpayers and tax professionals to use it. Multi-factor authentication can reduce the likelihood of identity theft by making it difficult for thieves to get access to sensitive accounts.

Users should check the security sec-

See **Authentication** on page 2

Authentication (continued from page 1)

tion in their online tax product account to make the change. It may be labeled as two-factor authentication or two-step verification or similar names.

Use of multi-factor authentication is especially important for tax professionals who continue to be prime targets of identity thieves. Of the numerous data thefts reported to the IRS from tax professional offices this year, most could have been avoided had the practitioner used multi-factor authentication to protect tax software accounts.

Thieves use a variety of scams – but most commonly by a phishing email – to download malicious software, such as keystroke software. This malware will eventually enable them to steal all passwords from a tax pro. Once the thief has accessed the practitioner's networks and tax software account, they will complete pending taxpayer returns, alter refund information and use the practitioner's own e-filing and preparer numbers to file the fraudulent return – a dangerous combination.

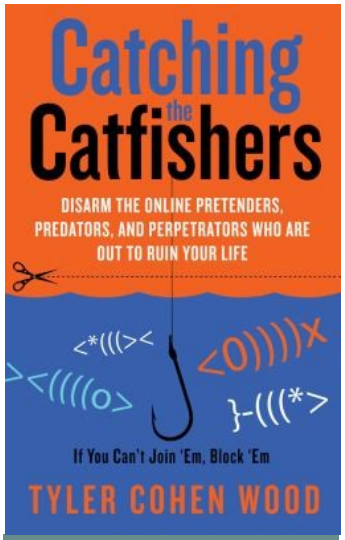
However, with multi-factor authentication, it's unlikely the thief will have stolen the practitioner's cell phone — blocking the ability to receive the necessary security code to access the account. This protects the tax pro's account information.

There are multiple options for multi-factor authentication. For example, taxpayers and tax practitioners can download an authentication app to their mobile device. These apps are readily available through Google Play or Apple's App Store. Once properly configured, these apps will generate a temporary, single-use security code, which the user must enter into their tax software to complete authentication. Use a search engine for "Authentication apps" to learn more.

Other options include codes that may be sent to practitioner's email or mobile phone via text but those are not as secure as an authentication app.

While no product is fool-proof, multi-factor authentication does dramatically reduce the likelihood that taxpayers or tax practitioners will become victims. Multi-factor authentication should be used wherever it is offered. For example, financial accounts, social media accounts, cloud storage accounts and popular email providers all offer multi-factor authentication options. ☐

Excerpted from IRS National Tax Security Awareness Week, Day 2: 2021 online tax preparation products to offer multi-factor authentication for taxpayers, tax pros | Internal Revenue Service



Available at www.rvl.info

Book—*Catching the Catfishers: Disarm the Online Pretenders, Predators, and Perpetrators Who Are Out to Ruin Your Life*

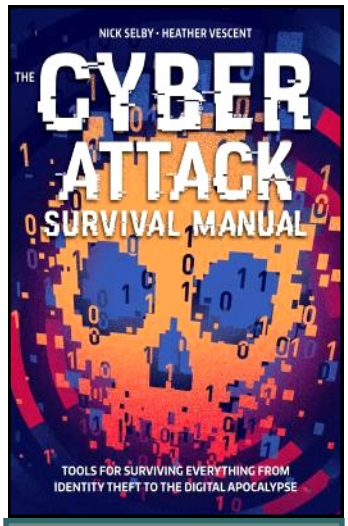
From the back cover: Your online identity is quickly becoming more crucial to your personal and professional success than in-person communications.
But most of us don't understand this digital Wild West and the dangers that lurk around every corner. Most of us are unaware of the digital bread crumbs that we leave behind with every post, and how easy it is for a person with malicious intent to harm us.
Catching the Catfishers shows you how to:

- Protect yourself and your children from online predators, cyber-stalkers, and chat-room bullies.
- Detect if someone is not who he or she claims to be.
- Learn what digital bread crumbs you leave behind and how to clean them up.

About the author: Tyler Cohen Wood is an expert in social media and cyber issues. She is a senior officer and a cyber branch chief for the Defense Intelligence Agency (DIA), within the Department of Defense (DoD) where she makes decisions and recommendations significantly changing, interpreting, and developing important cyber policies and programs affecting current and future DoD and Intelligence Community policies. She coauthored the textbook *Alternate Data Storage Forensics* and was featured in Best *Damn Cybercrime and Digital Forensics Book Period*. She previously worked for the DoD Cyber Crime Center as a senior digital forensic analyst, using her expertise in intrusion, malware analysis, and major crimes to bring about many successful prosecutions.

Book Spotlight— *Cyber Attack Survival Manual*

Tools for Surviving Everything from Identity Theft to the Digital Apocalypse



Available at www.rvl.info

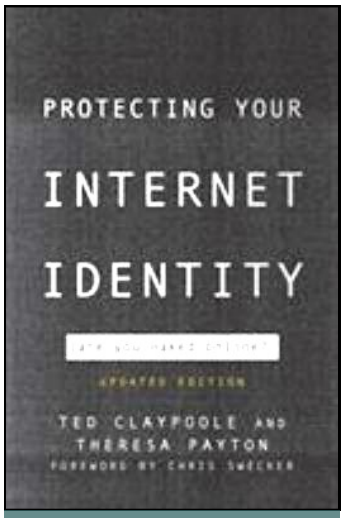
From the back cover: "Identity theft. Email hacks. Infrastructure attacks. Credit card fraud. Even murder for hire. All of these crimes can be committed with just a few clicks of a mouse. Cyber criminals can attack at any time, targeting you through a laptop, a smartphone, a television—even your doorbell or thermostat. The good news? You don't have to be a victim. In this comprehensive, practical, and fact-filled book, global security expert Nick Selby and futurist Heather Vescent give you the tools you need to protect your family, your privacy, your finances, and your reputation. Don't go online without it." ☐

About the authors:

Heather Vescent is a social scientist who studies trends to help people understand and take advantage of change. She is best known for her research on the Future of Transactions, which she presented at SxSW, Sibos, TedxZwolle, The Future of Money, Tomorrow's Transactions and other conferences around the world.

Nick Selby has nearly 20 years of cyber security and intelligence experience. The former Director of Cyber Intelligence and Investigations at the NYPD, he is currently Chief Security Officer at a New York City based trust company. He appears frequently in media including the New York Times, Washington Post, CNN, NPR, and Fox News discussing online security, terrorism, and more.

Book Spotlight— *Protecting Your Internet Identity*



Available at www.rvl.info

From the publisher

Staying Safe in an Increasingly Connected—and Dangerous—World

People research everything online – shopping, school, jobs, travel – and other people. Your online persona is your new front door. It is likely the first thing that new friends and colleagues learn about you. In the years since this book was first published, the Internet profile and reputation have grown more important in the vital human activities of work, school and relationships. This updated edition explores the various ways that people may use your Internet identity, including the ways bad guys can bully, stalk or steal from you aided by the information they find about you online. The authors look into the Edward Snowden revelations and the government's voracious appetite for personal data. A new chapter on the right to be forgotten explores the origins and current effects of this new legal concept, and shows how the new right could affect us all. Timely information helping to protect your children on the Internet and guarding your business's online reputation has also been added.

The state of Internet anonymity has been exposed to scrutiny lately, and the authors explore how anonymous you can really choose to be when conducting activity on the web. The growth of social networks is also addressed as a way to project your best image and to protect yourself from embarrassing statements. Building on the first book, this new edition has everything you need to know to protect yourself, your family, and your reputation online. ☐

Review: Helps readers understand the implications of online identities and how people may put themselves at risk professionally and personally.

—Grand Forks [Sd] *Herald*

There are thousands of new scams every year, and sometimes, it's challenging to keep up with all of them (we know, we try!).

However, if you can just remember these TEN TIPS, more than likely, you will be able to avoid most scams while protecting yourself and your family.

1. Never send money via gift card or wire transfer to someone you have never met face-to-face. Seriously, just don't ever do it. If they ask you to use wire transfer, a prepaid debit card, or a gift card, those cannot be traced and are as good as cash. Chances are, you won't see your money again. See the FTC video on how scammers try to convince you to pay. If someone is trying to convince you to pay this way, stop, get off the pHone or the computer, and file a complaint with the Federal Trade Commission (FTC). Report the activity to BBB Scam Tracker.

2. Avoid clicking on links or opening attachments in unsolicited emails. Links, if clicked, will download malware onto your computer, smart phone, tablet or what ever electronic device you're using at the time allowing cyber thieves to steal your identity. Be cautious even with email that looks familiar; it could be fake. Instead, delete it if it looks unfamiliar and block the sender.

3. Don't believe everything you see. Scammers are great at mimicking official seals, fonts, and other details. Just because a website or email looks official does not mean that it is. Caller ID is commonly faked.

Consider only connecting with people you already know. Imposters often get information about their targets from their online interactions, and can make themselves sound like a friend or family member because they know so much about you.

4. **Double check your online purchase is secure before checking out.** Look for the "https" in the URL (the extra s is for "secure") and a small lock icon on the address bar. Better yet, before shopping on the website, make certain you are on the site you intended to visit. Check out the company first at BBB.org. Read reviews about the quality of the merchandise, and make sure you are not buying cheap and/or counterfeit goods. Look for a brick and mortar address listing on the website itself and a working phone number. Take an extra step and call the number if it is a business you are not familiar with.

5. Use extreme caution when dealing with anyone you've met online. Scammers use dating websites, Craigslist, social media, and many other sites to reach potential targets. They can quickly feel like a friend or even a romantic partner, but that is part of the con for you to trust them.

6. Never share personally identifiable information with someone who has contacted you unsolicited, whether it's over the phone, by email, on social media, even at your front door. This includes banking and credit card information, your birthdate, and Social Security/ Social Insurance numbers.

7. Resist pressure to act immediately. Shady actors typically try to make you think something

See **BBB Tips** on page 8

Common Scams and Frauds

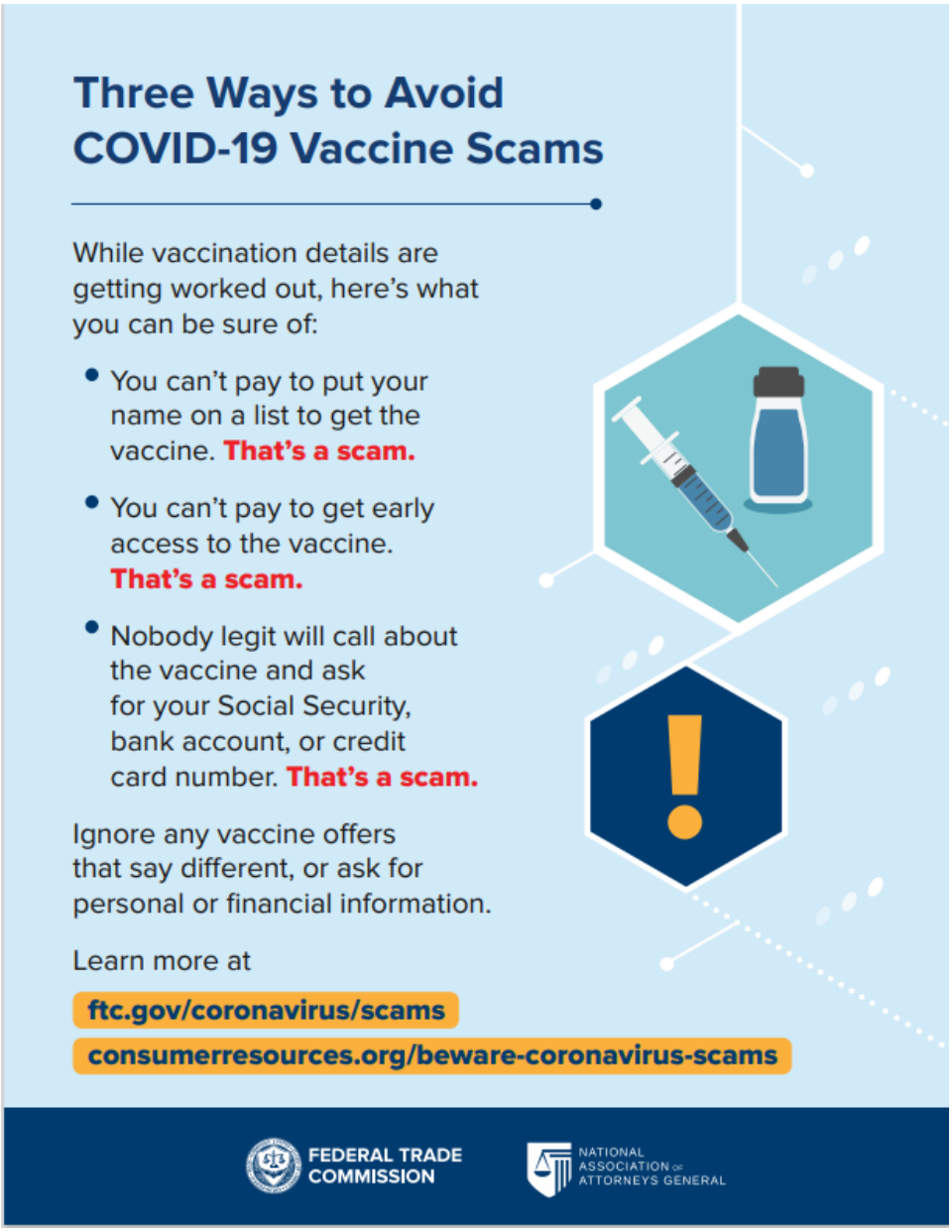
CORONAVIRUS SCAMS, RUMORS, AND PRICE GOUGING

During the coronavirus (COVID-19) pandemic, scammers may try to take advantage of you through misinformation and scare tactics. They might get in touch by phone, email, postal mail, text, or social media. Protect your money and your identity by not sharing personal information like your bank account number, Social Security number, or date of birth. Learn how to recognize and report a COVID vaccine scam and other types of coronavirus scams.

Common Coronavirus Scams

Scammers change their methods frequently. Current coronavirus scams include:

- **COVID-19 testing, vaccine, and treatment scams**—Don't trust offers to get early access to the approved vaccine. Be aware that scammers are also targeting Medicare recipients by offering COVID-19 testing in an attempt to steal personal information.
- **Charity scams**—Fake charities pop up during disasters. Scammer can also claim to be from real charities. Learn how to research charity claims and protect your money.
- **Checks from the government**—Scammers say they're from the IRS or another government agency and ask for your personal information or try to charge you fake fees for getting your stimulus check or offer you a way to get the money early.
- **FDIC and banking**—People pretend to call from the Federal Deposit Insurance Corporation (FDIC) or your bank and say your bank account or your ability to get cash are in danger and ask for your personal information.
- **Grandparent and military service member scams**—A scammer pretends to be a grandchild or a military service member who's sick or in trouble because of the coronavirus. They contact you asking to wire them money to pay for fake medical or travel expenses.



Learn about other types of coronavirus scams and listen to recordings of sample phone messages from scammers.

Continued on page 6

Report Coronavirus Scams

- Contact the National Center for Disaster Fraud hotline at 866-720-5721 or email disaster@leo.gov.
- Report a scam to the FBI at tips.fbi.gov.
- If it's an online scam, submit your complaint through the Internet Crime Complaint Center (IC3).

Coronavirus Rumors

Rumors, myths, and conspiracy theories about the coronavirus can be frightening and misleading. Go to FEMA's Rumor Control page to check out the real answers about the rumors you're hearing.

Report Price Gouging

During times of high demand, sellers may raise prices to a very high and unfair level on needed items like:

- Face masks
- Hand sanitizer
- Household or personal care items

This is called price gouging and it's illegal. If you suspect price gouging, report it to your state attorney general.

IDENTITY THEFT

Identity (ID) theft happens when someone steals your personal information to commit fraud.

The identity thief may use your information to apply for credit, file taxes, or get medical services. These acts can damage your credit status and cost you time and money to restore your good name.

Warning Signs of ID Theft

You may not know that you're the victim of ID theft immediately. You could be a victim if you receive:

- Bills for items you didn't buy
- Debt collection calls for accounts you didn't open
- Denials for loan applications

Potential Victims of ID Theft

Children and seniors are both vulnerable to ID theft. Child ID theft may go undetected for many years. Victims may not know until they're adults, applying for their own loans.

Seniors often share their personal information with doctors and caregivers. The number of people and offices that access seniors' information put them at risk.

Types of ID Theft

There are several common types of identity theft that can affect you:

- Tax ID theft—Someone uses your Social Security number to falsely file tax returns with the IRS or your state.
- Medical ID theft—Someone steals your Medicare ID or health insurance member number. Thieves use this information to get medical services or send fake bills to your health insurer.
- Social ID theft—Someone uses your name and photos to create a fake account on social media.

Prevent Identity Theft

Keep these tips in mind to protect yourself from identity theft:

- Secure your Social Security number (SSN). Don't carry your Social Security card in your wallet. Only give out your SSN when necessary.
- Don't share personal information (birthdate, Social Security number, or bank account number) just because someone asks for it.
- Collect mail every day. Place a hold on your mail when you are away from home for several days.
- Pay attention to your billing cycles. If bills or financial statements are late, contact the sender.
- Use the security features on your mobile phone.
- Update sharing and firewall settings when you're on a public Wi-Fi network. Use a virtual private network (VPN), if you use public Wi-Fi.
- Review your credit card and bank account statements. Compare receipts with account statements. Watch for unauthorized transactions.
- Shred receipts, credit offers, account statements, and expired credit cards. This can prevent "dumpster divers" from getting your personal information.
- Store personal information in a safe place.
- Install firewalls and virus-detection software on your home computer.
- Create complex passwords that identity thieves cannot guess. Change your passwords if a company that you do business with has a breach of its databases.
- Review your credit reports once a year. Be certain that they don't include accounts that you have not opened. You can order it for free from Annualcreditreport.com.
- Freeze your credit files with Equifax, Experian, Innovis, TransUnion, and the National Consumer Telecommunications and Utilities Exchange for free. Credit freezes prevent someone from applying for and getting approval for a credit account or utility services in your name.

Report Identity Theft

Report ID theft to the Federal Trade Commission (FTC) online at IdentityTheft.gov or by phone at 877-438-4338.

If you report ID theft to the FTC online, you will receive an identity theft report and a recovery plan. Create an account on the website to:

- Update your recovery plan
- Track your progress
- Receive prefilled form letters to send to creditors ☐

Excerpted from Scams and Frauds | USAGov

CHARITY NAVIGATOR
Your Guide To Intelligent Giving

***Charities that cause concern from our experts*—Charity Navigator (CN) Advisory System** is a platform that helps donors make informed giving decisions by providing them with information about particular charities—such as alleged or confirmed illegal activity or ethnicity breaches—that may influence their decision to donate. To learn more about this system, you can read the methodology on our website.

Information about the conduct or operations of a charity or a fraudulent organization posing as a charity that comes to the attention of Charity Navigator is reviewed by the CN Advisory Issuance Committee (CNIAC).

The CN Advisory System categorizes Advisories into three levels of concern: Low, Moderate, High. Issues regarding the conduct, operations, or management of a charity or an alleged charity that could result in a CN Advisory may include, but are not limited to:

Low Concern Advisory

- A media outlet, nonprofit expert or other third-party evaluation (typically other than a governmental or criminal justice system entity) reports on credible allegations of improper conduct or operations at a charity.
- Charities affiliated with organizations that have a High or Moderate Concern CN Advisory.
- Reports that federal, state, or local funding for a charity has been, or may be, cancelled or suspended, including because of alleged misconduct.

Moderate Concern Advisory

- Unconfirmed allegations of fraud (mail, insurance or tax fraud), embezzlement, conspiracy, any type of abuse (animal or other), and any other type of illegal or improper conduct or organizational mismanagement.
- The receipt of an incomplete or inaccurate Form 990 and the charity's failure to provide an adequate explanation or an amended Form 990. Examples that have led to a CN Advisory include charities that do not complete the schedule of expenses or that do not report their fundraising expenses.
- Audits that contain a qualified opinion and/or an "Emphasis of Matter Regarding Going Concern."

High Concern Advisory

- An alleged charity that is soliciting funds from the public.
- Confirmed allegations of fraud (mail, insurance or tax fraud), embezzlement, conspiracy, any types of abuse (animal or other), and any other type of illegal or improper conduct or organizational mismanagement.

AARP
Fraud Watch Network

Stay One Step Ahead of the Scammers

Every year, thousands of Americans are affected by fraud and scams—but you don't have to be one of them! Sign up for biweekly Watchdog Alerts to have news on the latest scams delivered right to your inbox.

Requires email address or cell phone number.

FEDERAL TRADE COMMISSION
Consumer Information

Sign up for FTC Consumer Alerts for email updates for scam alerts, Don't have email, visit their website for their Most Recent Scam Alert or browse scams by topic including (but not limited to):

Car Buying Scams	Family Emergency Scams	Job Scams
Charity Scams	Free Trial Scams	Phishing Scams
Debt & Credit Scams	Gift Card Scams	Phone Scams
Fake Check Scams	IRS Impersonators	Romance Scams

Salem Public Library

28 E Main Street
Salem VA 24153

Phone: 540-375-3089
Fax: 540-389-7054
Email:
library@salemva.gov

Roanoke Valley Libraries Online Library Catalog www.rvl.info

Roanoke Valley Libraries e-Books & e-Audiobooks rvl.overdrive.com

WE'RE ON THE WEB!

HTTPS://WWW.SALEMVA.GOV/DEPARTMENTS/SALEM-PUBLIC-LIBRARY

ABOUT THIS NEWSLETTER: This free, weekly (during the pandemic) newsletter is intended for people over 50 and their caregivers.

SUBSCRIPTION INFORMATION: If you would like to subscribe to our newsletter, please let us know by either:

- Calling the library between 10:00 a.m. and 4:00 p.m. each day OR
- Email us at library@salemva.gov OR

Print copies will be available in our lobby between 10:00 a.m. and 4:-00 p.m. each day and we will post a link on our website to view this newsletter online. Archived versions of this newsletter are posted on our website on the Adult Resources page.

LIBRARY SERVICES/EVENTS BEING OFFERED AT THIS TIME:

CONTACT FREE PICK-UP is available in our front lobby every day from 10:00 a.m. to 4:00 p.m. for picking up requested items. Please call before heading to the library so that we can check out your items before you get here. *Thank you!*

***LEAVE IT TO A LIBRARIAN* For Adult Fiction**: *The library is closed and you don't want to spend hours browsing the online catalog?* Call us, email us, or click the link on our website home page to give a hint or two (genre, authors you like). Tell us how many books you want. We'll fill a bag and leave it in the front foyer for you.

SOCIALIZE WITH US! ON FACEBOOK, GOODREADS, OR INSTAGRAM—Click on the icons near the bottom of our website home page.

Scan this QR code to see our calendar of events

BBB Tips (continued from page 4

is scarce or a limited time offer. They want to push victims to make a decision right now before even thinking through, asking family members, friends or a financial advisor. Sometimes, they'll advise you to avoid contacting anyone and to just trust them. While high-pressure sales tactics are also used by some legitimate businesses, it typically isn't a good idea to make an important decision quickly.

8. Use secure and traceable transactions. Do not pay by wire transfer, prepaid money card, gift card or other non-traditional payment method (see number one on page 4). Say no to cash-only deals, high pressure sales tactics, high upfront payments, overpayments, and handshake deals without a contract. Read all of the small print on the contract and make sure to understand what the terms are.

9. Whenever possible, work with local businesses. Ask that they have proper identification, licensing, and insurance, especially contractors who will be coming into your home or anyone dealing with your money or sensitive information. Review Business Profiles at BBB.org to see what other people have experienced.

10. Be cautious about what you share on social media. Consider only connecting with people you already know. Check the privacy settings on all social media and online accounts. Imposters often get information about their targets from their online interactions, and can make themselves sound like a friend or family member because they know so much about you. Then, update and change passwords to passphrases on a regular basis on all online accounts. ☐

Excerpted from BBB Tips: 10 Steps to Avoid Scams